Desafío Técnico ML - Gestión de Incidentes

1. Descripción del Incidente

Durante la implementación de la infraestructura en AWS, se detectó un problema de conectividad entre la instancia EC2 y el servicio de almacenamiento Amazon S3. Este fallo impidió la ejecución de los respaldos automáticos de archivos desde la instancia hacia el bucket S3.

El objetivo de este documento es detallar el análisis del problema, la solución implementada y las medidas preventivas adoptadas.

2. Pruebas Realizadas

Para diagnosticar el problema, se realizaron las siguientes pruebas:

1. Verificación de conectividad desde EC2 a S3:
    - Se ejecutó aws s3 ls s3://desafio-tecnico-ml-web/ desde la instancia EC2.
    - El comando arrojó un error 403 Forbidden, indicando problemas de acceso.
2. Revisión de Security Groups:
    - Se detectó que la regla de egreso de la instancia EC2 no permitía tráfico saliente a Internet, bloqueando la comunicación con S3.
3. Validación de IAM Policies:
    - Se comprobó que la política IAM asociada a la instancia EC2 tenía los permisos correctos (s3:PutObject y s3:ListBucket).
4. Monitoreo en CloudWatch Logs:
    - Se observaron múltiples intentos fallidos de conexión a S3 con errores 403 Forbidden.

3. Análisis de Causas

El problema fue causado por una configuración incorrecta en el Security Group asociado a la instancia EC2:

- La regla de salida del Security Group solo permitía tráfico hacia puertos específicos internos.

- No se había configurado una regla para permitir tráfico HTTPS (puerto 443), necesario para conectarse a S3.

4. Solución Implementada

Para corregir el incidente, se realizó el siguiente ajuste:

1. Modificación del Security Group:
    - Se agregó una regla de egreso para permitir tráfico saliente por el puerto 443 (HTTPS) hacia Internet, permitiendo la comunicación con Amazon S3.

Después de aplicar este cambio, se realizó una prueba con aws s3 ls y se confirmó que la instancia podía acceder correctamente al bucket.

5. Medidas Preventivas

Para evitar que este problema vuelva a ocurrir, se han tomado las siguientes medidas:

1. Validaciones antes de la implementación:
    - Se revisarán los Security Groups antes de aplicar cambios con Terraform.
2. Monitoreo y alertas en AWS CloudWatch:
    - Se configuraron métricas en CloudWatch Logs para detectar intentos fallidos de conexión a S3.
    - Se creó una alerta en Amazon SNS, que envía notificaciones por correo electrónico si se registran errores 403 Forbidden en los intentos de conexión.

6. Conclusión

La rápida corrección de la regla en el Security Group permitió restablecer la conectividad con S3 y asegurar la ejecución de los respaldos sin problemas. La implementación de monitoreo en **CloudWatch** y alertas en **SNS** permitirá detectar este tipo de fallos en el futuro de manera proactiva.